BCS03156

SEPARATION OF COPY PROTECTION RULES FOR DIGITAL RIGHTS MANAGEMENT

Field of the Invention

[0001] This invention relates to digital rights management (DRM), and more particularly to methods and systems for providing copy protection of digital content within an authorized domain. Such a domain can comprise, for example, a home network that is licensed to play content such as movies, games, music and the like on various different entertainment appliances coupled to the network.

Background of the Invention

[0002] Providers of digital content, such as music on compact discs (CD) and movies on digital versatile discs (DVD) often desire protection from unauthorized copying of the content. Such content can also be streamed to users via networks such as cable and satellite television plants, as well as over the Internet. Existing copy protection rules, such as those defined by the Society of Motion Picture and Television Engineers (SMPTE), generally do not take into account the existence of authorized domains, where devices (televisions, DVD players, game consoles, personal computers, and the like) owned by a single authorized user can securely exchange content.

[0003] Known copy protection standards include states such as "Copy One Generation", "Copy No More", and "Copy Free." Such states make sense when content is communicated over an external unprotected interface or stored on media such as a CD or DVD. However, these standards can make it very difficult for an authorized (e.g., licensed) user to use the content on different devices on that user's authorized domain (e.g. home network).

[0004] It would be advantageous to provide copy protection systems and methods that maintain an adequate level of protection for content and service providers, while allowing the content to be easily copied or moved within a protected authorized domain. It would be further advantageous for such systems and methods to maintain compatibility with traditional copy protection solutions (e.g., CGMS - "Copy Generation Management System"). This would allow external devices, such as digital televisions or computer monitors, to continue to display the content in accordance with the traditional copy protection rules.

[0005] It would be still further advantageous to allow content users to legally share content over protected interfaces (e.g., on-line or removable media). As it is rarely acceptable to allow a user to share pay content with everyone, it would also be advantageous to enable a list of authorized domains to be specified for the sharing of content.

[0006] The present invention provides systems and methods for implementing digital rights management having the aforementioned and other advantages.

SUMMARY OF THE INVENTION

[0007] In accordance with one aspect of the invention, a method is provided for managing rights to content within an authorized domain. In a single authorized domain, where a plurality of domain interfaces are protected using a common rights management system, the method specifies if a copy of particular content is allowed to be provided on all devices or only on specific devices coupled to the domain via the interfaces. Copy protection information, with separately defined rules for outputs to external devices not protected by the common rights management system, is also specified.

[0008] Such a method may also specify whether particular content may be copied or moved to another domain protected by a rights management system. A number of rendering devices permitted to render the content simultaneously may also be specified.

[0010] Another aspect of the invention provides a ruleset for use in managing rights to content within an authorized domain. The ruleset can include, for example, rules defining capabilities of devices associated with the domain, rules defining persistent entitlements, and copy protection rules.

[0011] Rules defining capabilities of devices associated with the domain can include, for example, one or more of a device security level, a designation of whether a device supports secure time, a designation of codecs associated with a device, a designation of watermarks a device can check, and a designation of fingerprints a device can provide.

[0012] Rules defining persistent entitlements can include, for example,rules for forwarding content on legacy analog, digital compressed and digital uncompressed interfaces, for peer-to-peer content sharing, content playback controls, limit on the number of simultaneous devices rendering the content, fingerprint algorithms and required device capabilities to render the content. Copy protection rules can include, for example,

legacy device rules for restricting copies over at least one of an analog, compressed digital or uncompressed digital interface. Copy protection rules can also include rules for non-persistent content to be displayed within the authorized domain.

[0013] In another aspect, the invention provides a system for distributing content to end users. A network is used for the delivery of licensed content to a home network. The home network can be an authorized domain where a plurality of domain interfaces are protected using a common rights management system. Licensed content is associated with rights data specifying whether the content is allowed to be provided on all devices or only specific devices coupled to the domain via the interfaces. Copy protection information is provided for outputs from the home network to external devices not protected by the common rights.

[0014] An additional network can be coupled to the home network for receiving the licensed content. In such an embodiment, the additional network can also be an authorized domain, where all interfaces thereto are protected using the common rights management system.

BRIEF DESCRIPTION OF THE DRAWINGS

[0015] For a further understanding of the present invention, reference will be made to the following detailed description of the invention which is to be read in association with the accompanying drawings, wherein:

[0016] FIG. 1 is an example screen shot showing a session rights element;

[0017] FIG. 2 is an example screen shot showing a rule element;

[0018] FIG. 3 is an example screen shot showing a purchase option element;

[0019] FIG. 4 is an example screen shot showing a subscription element;

[0020] FIG. 5 is an example screen shot showing a blackout element;

[0021] FIG. 6 is an example screen shot showing a generic rating element;

[0022] FIG. 7 is an example screen shot showing a selection element;

[0023] FIG. 8 is an example screen shot showing a user authorization element;

[0024] FIG. 9 is an example screen shot showing a persistent entitlements element;

[0025] FIG. 10 is an example screen shot showing a rule set element;

[0026] FIG. 11 is an example screen shot showing a redistribution element;

[0027] FIG. 12 is an example screen shot showing a playback element;

[0028] FIG. 13. is an example screen shot showing an option cost element;

[0029] FIG. 14 is an example screen shot showing a copy protection rules element; and

[0030] FIG. 15 is a block diagram of an example network implementation of the invention.

DETAILED DESCRIPTION OF THE INVENTION

[0031] The growing interest in streaming distribution of multimedia content over Internet Protocol (IP) networks brings a need for secure delivery of such content to legitimate customers. For purposes of the present disclosure, the term IP Rights Management (IPRM) encompasses conditional access as well as the various issues surrounding persistent access, defined as access to content after the customer has received and decrypted it the first time. Persistent access can be accommodated, for example, by storing the decrypted content on a hard drive provided, e.g., in a Personal Video Recorder (PVR) or Personal Computer (PC). IPRM, which is within the realm of Digital Rights Management (DRM), can be viewed as a generalization of conditional access technology.

[0032] The present disclosure describes Extensible Markup Language (XML) interfaces that are used by external systems in order to use services provided by the IPRM system. These XML documents need to be processed and understood by Caching Servers that deliver content to viewers (viewers comprise one category of IPRM clients) as well as by the IPRM clients that need to follow copy protection rules for the content that is being rendered and/or persistently stored.

[0033] Extensible Markup Language describes a class of data objects called XML documents and partially describes the behavior of computer programs which process them. XML is an application profile or restricted form of SGML, the Standard Generalized Markup Language (ISO 8879). By construction, XML documents are conforming SGML documents.

[0034] XML documents are made up of storage units called entities, which contain either parsed or unparsed data. Parsed data is made up of characters, some of which form

character data, and some of which form markup. Markup encodes a description of the document's storage layout and logical structure. XML provides a mechanism to impose constraints on the storage layout and logical structure.

[0035] A software module called an XML processor is used to read XML documents and provide access to their content and structure. It is assumed that an XML processor is doing its work on behalf of another module, called the application.

[0036] The following acronyms are used herein:

API	Application Programming Interface
ASN.1	Abstract Syntax Notation One
CA	Conditional Access or Certificate Authority
CGMS	Copy Generation Management System. This may be an analog system (CGMS-A) or a digital system (CGMS-D)
DRM	Digital Rights Management
ECM	Entitlement Control Message
EMM	Entitlement Management Message
IP	Internet Protocol
IPPV	Instant Pay-Per-View
IPRL	Internet Protocol Rights Language
IPRM	Internet Protocol Rights Management
KDC	Key Distribution Center
OCS	Origin Content Server
PKI	Public Key Infrastructure
PBQ	Pay-By-Quality
PBT	Pay-By-Time
PPV	Pay-Per-View
SRO	Session Rights Object

SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
VOD	Video On Demand
XML	Extensible Markup Language

[0037] The following terms are used herein:

[0038] **Content Provider** An entity that creates, licenses, aggregates and/or distributes content to the Cache Servers. A content provider does not typically consume content. A content provider is responsible for specifying content access rules and possibly user selection if the user actually makes the purchase at the content provider's web portal. Otherwise, user selection is made by the Confirmation Server.

[0039] **Cache Server** An intermediate entity that stores and redistributes content to Consumers and optionally to other Cache Servers. Besides streaming content to viewers, it also enforces the content access rules against the user selection and user entitlements.

[0040] **Confirmation Server** An application facilitating the creation of a session rights object.

[0041] **Consumer** An entity such as an end-user that consumes content obtained from a Cache Server and optionally, if permitted by the copyright holder, redistributes content to other Consumers in the system. The user is given a set of entitlements by the provisioning center that are used to determine the satisfaction of content access rules. When a user makes a purchase of specific content, the user's selection is included in the Session Rights object.

[0042] **Entitlements** A set of authorization attributes that allow users to access content.

[0043] **Provisioning Center** An application that registers a new consumer (e.g. Viewer) with the network, provisions it with the Key Distribution Center (KDC) and creates a set of entitlements for the new user.

[0044] **Session Rights Object** A signed version of content access rules for a given piece of content and specific user's purchase option selection.

[0045] **Ticket** A token of trust issued to a viewer by the KDC in order to access content at a particular caching server. It also includes the user's entitlements.

[0046] **Viewer** A consumer of video content.

[0047] A main purpose of the disclosed IPRM system is to provide digital rights management functions such as authentication, privacy, security, integrity and access control tools to any multimedia streaming network based on IP protocols. The system supports point-to-point (VOD) and multicast delivery of content. Additional features relate to persistent (i.e., stored) content rights management, such as copy protection.

[0048] The system can be based purely on software protection, with a limited trust placed upon the clients. However, other implementations are possible, including those in which a hardware security module is provided. Such a hardware security module may be optional. Alternatively, hardware security may be mandatory to obtain rights to high quality content from copyright owners requiring high security levels.

[0049] A Session Rights XML document can be generated by a content provider or any other entity (e.g. a Confirmation Server) that provides final interaction with the end-user. The content of the Session Rights document may be encoded in a Session Rights Object. A Rights element is the root element of the Session Rights document. It is a sequence of Content and Selection elements, which are required, and Provider and Rule elements, which are optional.

[0050] An authorization XML document can be maintained by the Provisioning Server and included in each ticket given to a Viewer by the KDC. A Rights Manager module on the Caching Server can be provided to evaluate the rules and user selection against the authorization data in the ticket to allow or disallow access to the specified content.

[0051] Each XML document may consist of a root element and a set of nested elements.

[0052] Figure 1 is a computer screen shot illustrating one possible implementation of a session rights element 10. Content element 12, which is part of the session rights element 10, uniquely identifies the content associated with this set of session rights. A "format" attribute can be provided as part of the content element to indicate the format in which the content identification is specified (e.g. URL, ISBN, etc.). URL, for example, can be the default. An "id" attribute can be used to specify the unique content identifier. A 'protected' attribute may be provided to indicate whether the associated content is encrypted (e.g., during the pre-encryption phase and/or when it is delivered to a consumer). This attribute can, for example, be set to 'Y' as a default option, indicating that the content is encrypted both during pre-encryption and when delivered. Otherwise, the associated content is unprotected.

[0053] A provider element 14 can optionally specify a ProviderID ("pid" attribute) and the provider name as a text string.

[0054] The rule element 16 specifies a set of rules for the content specified by the content element 12. An "extern" attribute can be provided for the rule element 16 to specify whether the rules are defined in this document (e.g., value "false") or in an external document (e.g., value "true"). The default value can be, for example, "false." The rules do not change often and can be cached, for instance at a Caching Server, where the user can retrieve protected content. In order to minimize bandwidth overhead, the "extern" attribute may be set to "true" when the rules are being cached. Such an

implementation will significantly reduce the size of each Session Rights Object (SRO).

[0055] A selection element 18 specifies a purchase selection made by a user, on whose behalf this Session Rights document is presented. An "optionID" attribute can be provided for the selection element 18 to identify a particular PurchaseOption defined within the Rule element that was selected by the user. Each option may be associated with different copy protection rules for persistent or non-persistent content. An "extern" attribute may also be provided for the selection element 18, to specify whether the selection is defined in this document (e.g., value "false") or in an external document (e.g., value "true"). The default value may, for example, be "false." A "deviceBound" attribute may also be provided for the selection element 18. If, for example, this attribute is set to 'Y', the content will not be shared outside the access device. If it is set to 'N', then the content will be shared across the user's authorized domain. If this attribute is not specified within the selection element 18, the system can be implemented to check the same "deviceBound" attribute inside the persistent entitlements to find out whether or not to share particular content across the authorized domain. The deviceBound attribute affects how blackout verification is performed. For example, if the content is not shared outside the access device, then the blackout check may only apply to the locations (listed inside Authorization Data) that have an "AccessPoint" attribute set to "Y." Otherwise, all locations listed in the Authorization Data will need to be checked. The value of this attribute must be consistent with the persistent entitlements that are associated with the user selection.

[0056] The rule element 16 is illustrated in greater detail in Figure 2. This element specifies all access rules associated with the specified content. It is a choice of one or more of the available rules. If the rule element is not specified, it may be assumed that the content is:

- free;
- not blacked out anywhere;
- has no rating associated with it;
- not available for subscription; and
- no particular level of security is required to access it.

In one possible implementation, in order to get access to such content, a purchase element in the user Selection must be set to FREE.

[0057] The PurchaseOption element 20 defines copy protection rules or DRM rules for persistent data associated with a specific option for purchasing this content. This option is also associated with a price and a list of subscription services under which this option may be selected for free or at a decreased cost. Multiple PurchaseOption elements may be included to indicate different options for the user to purchase the content. Some of the options may restrict the purchase to only initial rendering of the content, while other options may allow the user to save a copy of the content with varying DRM rules.

[0058] The "optionID" of the Selection element 18 (Figure 1) specifies the ID of the purchase option that was selected by the user. Typically, if an Origin Server generated a full set of Session Rights with both rules and user selection, there would only be a single PurchaseOption element included in the rules, which is the one selected by the user. This methodology is useful in conserving bandwidth. But if the Origin Server generates only the user selection while rules are cached on a Caching Server, the rules would typically include all PurchaseOption elements associated with this content. The PurchaseOption element is described in greater detail below, in connection with Figure 3.

[0059] A Blackout element 22 provides a mechanism for geographically restricting access to given content. It provides the ability to define an area specified by a list of country codes or other types of location designators where the content is or is not allowed. The Blackout element is described in greater detail in connection with Figure 5. This rule will be evaluated against the list of LocationGroups in an Authorization Data document described hereinafter.

[0060] A GenericRating element 24 specifies the content rating level for a particular rating scale or standard (e.g., MPAA rating, TV rating, etc.). This element can be repeated multiple times in order to define the rating levels for multiple rating scales. The GenericRating element is described in greater detail in connection with Figure 6. The rule (e.g., rule 16) which includes the GenericRating element 24 will be evaluated against a GenericRating element in the Authorization Data document discussed below, representing a user rating ceiling. In one possible embodiment, the ceiling must be equal to or higher than the content rating. This rule can be overridden by an Override element in the Selection element, as described in greater detail below in connection with Figure 7.

[0061] Fingerprint elements 26 shown in Figure 2 specify a list of fingerprint algorithms that may be applied to content being sent to a client. In a preferred embodiment, if at least one fingerprint element is present, one of the fingerprint algorithms must be applied by the streaming server.

[0062] DeviceCapabilities element 28 specifies security requirements for a consumer device receiving the content. Some of these security requirements can apply to content rendering, while others may apply when a device makes a persistent copy of the content. For content rendering, one or more of the following attributes can be provided:

- securityLevelToRender attribute, which specifies the minimum security level of the content rendering device.

- codecInSecureHW attribute, which is a flag that when provided at a specified state (e.g., true ('Y')) requires a rendering device to decompress content inside secure hardware.

- WatermarkInSecureHW attribute, which is a flag that, e.g., when true ('Y'), requires a rendering device to perform watermark detection inside secure hardware.

- FingerprintInSecureHW attribute, which is a flag that, e.g., when true ('Y') requires a rendering device to insert a fingerprint inside secure hardware.

For copying, the following attribute can be provided:

- SecurityLevelToCopy attribute, which is the minimum security level of the destination device that is getting a persistent copy of the content. This rule will be evaluated against the SecurityLevel attribute of the client ticket.

[0063] As indicated in Figure 2, one or more PurchaseOption elements are included in the Rule element. A PurchaseOption element is illustrated in greater detail in Figure 3. One element of the PurchaseOption element is a GenericRights element 30. This element has no type when directly present and indicates that the actual copy protection rules or rights associated with persistent content are specified in a different XML document. The GenericRights element is also a substitution group in which the substitution elements can comprise:

- CopyProtectionRules – defines copy protection rules associated with content which is not saved persistently, but could be forwarded to various digital and

analog outputs. This element is defined in a separate XML schema discussed hereinafter. It is a subset of the rules defined in the PersistentEntitlements.

- PersistentEntitlements – content usage rules associated with a persistent copy of the content. The presence of this element indicates that the content will either be downloaded or recorded by a client device during a streaming session. This element is defined in a separate XML schema discussed hereinafter.

[0064] A Cost element 32 associated with the PurchaseOption element 20 specifies the price of the content. A "currency" attribute specifies the currency expressed as a 3-letter acronym defined by ISO 4217. US dollar can, for example, be the default value. If a different currency representation is needed in the future, the "format" attribute can be used to specify other formats. This element is not applicable when content is made available on subscription basis only.

[0065] If the Cost element 32 is not specified, the content cannot be purchased and may be available for subscription. If the Subscription element (discussed below) is not specified either, the content is assumed to be free of cost.

[0066] Additional nested elements can be provided to specify different ways to buy the content. For example, a OneTimePay element can be provided to specify the price for a pay-per-view purchase mechanism. The "price" attribute can specify the cost for accessing this content.

[0067] A PBT element can be used to provide a mechanism to purchase content at time increments. An "increment" attribute can be provided to specify the time interval (in minutes) that the "price" is associated with. For instance, if the "price" is 95 cents and the increment value is thirty, the user will be charged 95 cents for each thirty minutes that the content is viewed. This rule will be checked against the Payment element in the Selection element 18 (Figures 1 and 7) and evaluated against the Pay element

(Figure 8) in the Authorization Data document, which represents the user's ability to pay for content.

[0068] Table 1 defines the relationship between elements of the PurchaseOption (in columns) and user Selection (in rows). When a particular value of Selection is present, the value YES specifies that the element of PurchaseOption in that column must be present and will be evaluated. The value N/A specifies that the corresponding element may be present but will not be used for evaluating access rights. The value NO means that the rule must not be present. The value DENIED means that access will be denied. In addition, the rightmost column shows the required value of the Pay element from the user authorization.

Table 1 – Rule Matching

Rule & Selection	Subscription Group	Cost-OneTimePay	Cost-PBT	Neither	Authorization: Pay
SUBSCR	YES	N/A	N/A	DENIED	Depends (see below)
OneTime Pay	N/A	YES	N/A	DENIED	INDIVIDUAL
PBT	N/A	N/A	YES	DENIED	INDIVIDUAL
FREE	NO	NO	NO	YES	N/A

[0069] If the Payment element (Figure 7) of the user selection is set to SUBSCR, the selected PurchaseOption 20 must contain one or more SubscriptionGroups 34. If there is at least one matching SubscriptionGroup without an IncrementalCost element 38, then the Pay element (Figure 8) in the user selection will be ignored. Otherwise, the value of the Pay element must be INDIVIDUAL. If none of the Subscription or Cost rules is specified, the content can be accessed only if the user Selection is set to FREE.

[0070] SubscriptionGroup 34 includes the following two elements:

- aSubscription - this element (36) specifies a list of services on which this piece of content is available for subscription, and is described in more detail in connection with Figure 4. Evaluation will be made against the list of aSubscription elements in the Authorization Data document (Figure 8) if the user selects the "SUBSCR" purchase option. If the user has at least one of the provider/service pairs in his entitlements, he will be granted access to the service (assuming that other rules, such as blackout and rating, are satisfied as well).

- IncrementalCost - this is an optional element (38) associated with a particular aSubscription element and indicates that there is still an amount that needs to be paid when the content is obtained through a subscription to one of the specified services. The "currency" and "format" attributes are the same as the "currency" and "format" attributes for the Cost element 32 of the PurchaseOption 20 described above. The "price" attribute specifies the (possibly reduced) cost for the content when it is obtained through this subscription.

[0071] The aSubscription element specifies a list of services on which a piece of content is available for subscription, as illustrated in Figure 4. Because there are multiple methods for identifying service providers and services, aSubscription is an abstract placeholder for a specific subscription element. The substitution elements for aSubscription are:

- SubscriptionID (40) – a list of two-byte unsigned integers representing service identifiers. This element also has an optional "provider" attribute that is a two-byte unsigned integer that identifies a provider. The reason the provider attribute is optional is because in some cases, service identifiers may be globally unique and may already imply a specific service provider.

- SubscriptionName (42) – a list of service names separated, e.g., by white space. In such an embodiment, each name may not itself contain white space. This

element also has an optional "provider" attribute that is the provider name (with no white space characters). In the case that service names are globally unique or already imply a specific provider, the provider attribute may be omitted.

- SubscriptionNumber (44) – a list of concatenated provider and service identifiers (two bytes for provider, two bytes for service).

[0072] It is noted that the number of bytes for the various elements and attributes disclosed herein is not meant to be limiting, and other implementations can be made within the scope of the present invention.

[0073] The Blackout element is illustrated in Figure 5. It comprises a sequence of locations where the content may or may not be viewed, depending on the value of a "restriction" attribute. The "restriction" attribute specifies whether the content is blacked out (i.e. disallowed) inside the specified geographic area (e.g., value IN) or outside of the area (e.g., value OUT). A "buyThru" attribute specifies whether the content can be purchased when the user would otherwise be blacked out. This is useful for content distributed on a subscription basis.

[0074] Each element of the Blackout sequence is a substitution group, needed to accommodate different types of location codes. The element aLocation (50) is an abstract placeholder for a specific location element. The substitution elements for aLocation are:

- **Country** (52) – a list of tokens separated by white space, where each token identifies a country as a two-character country code defined in "ISO3166" (the default value of the "format" attribute – other formats may be supported in the future).
- **DVDRegion** (54) – location specified by a list of DVD region codes separated by white space. The possible region codes are:

- **1** = U.S., Canada, U.S. Territories
- **2** = Japan, Europe, South Africa, and Middle East (including Egypt)
- **3** = Southeast Asia and East Asia (including Hong Kong)
- **4** = Australia, New Zealand, Pacific Islands, Central America, Mexico, South America and the Caribbean
- **5** = Eastern Europe (Former Soviet Union), Indian subcontinent, Africa, North Korea and Mongolia
- **6** = Peoples Republic of China
- **7** = Reserved
- **8** = Special international venues (airplanes, cruise ships, etc.)

- **PostalCode** (56) – a list of tokens separated by white space, where each token is a postal code location (e.g. ZIP code in US). It has an optional Boolean attribute "long" that specifies if the postal code is expressed in long form (e.g., 9-digit US ZIP code instead of a 5-digit one). If this attribute is not present, the short form is assumed. An optional "country" attribute specifies a country within which the postal codes are located. If the country is not specified, US is assumed. There is also an accompanying optional "format" attribute that specifies the type of the country code used in the value of the "country" attribute. The default value for "format" is "ISO3166".

[0075] The GenericRating element 24 specifies a content rating, as illustrated in Figure 6. GenericRating element is of type NMTOKEN and has the following possible values: LEVEL0, LEVEL1, LEVEL2, LEVEL3, LEVEL4, LEVEL5. GenericRating may be used as a custom content rating scale where the meaning of each level is the same in both the Session Rights and in the Authorization Data XML documents. Because there

are multiple rating scales, GenericRating is also a substitution group. The substitution elements for GenericRating are:

- **DVBRating** (60) – a positive integer between 3 and 18 that represents a minimum allowable age of the Viewer.
- **MPAARating** (62) – a string with no white space that represents one of the MPAA rating levels.
- **TvRating** (64) – a string with no white space that represents one of the North American TV rating levels.

[0076] It is possible to have multiple content rating elements in both Session Rights and Authorization Data XML documents. In that case, pairs of content rating elements from Session Rights and Authorization Data that are of the same type must be compared. For example, MPAARating element 62 in Session Rights would be compared to an MPAARating element in Authorization Data. If the rating ceiling set in Authorization Data is not exceeded for every such pair of rating elements, then the content rating check passes. If both Session Rights and Authorization Data have content rating elements but none of them have matching types, then the content rating check passes as well.

[0077] The Selection element 18 illustrated in Figure 7 specifies user selections related to the consumption or purchase of the selected content. It is a sequence of the following elements:

- **Payment element** (70) - specifies the purchase option the user has selected in order to obtain access to the content. The following values are defined.
  - **FREE** – the content is free
  - **SUBSCR** – the user has a subscription to the service

- **ONE-TIME-PAY** – the user selected the option to buy the content based on a single payment (no subscription)
- **PBT** – the user selected the option to buy the content on pay-by-time basis

- **Override element** (72) - specifies whether the user has overridden his rating ceiling when he ordered the content (e.g. provided a password or PIN code to the purchase or confirmation server). The value of this element specifies what rule was overridden, meaning that the rule is not going to be enforced. RATING is an example of a value that can be supported.

[0078] The Authorization element 80 of Figure 8 is the root element of the User Authorization Data document. It can include a sequence of several optional elements. These are purchasing capability (Pay element), user location (Country element), user subscription (Subscr and SubscrList elements), content rating ceiling (Rating element) and an element of type "any".

[0079] The Authorization element has several attributes:

- **principal** - a unique identifier of an end-user client who is requesting the specified content. This attribute is required so that it can be used for billing purposes, for instance.
- **operator** – an optional attribute identifying the network provider (MSO, ISP, etc.) of the end-user identified by the principal name above.

[0080] The Authorization element is also a sequence of the following elements:

- **Pay** element 82 specifies a user's ability to pay for content. The following values for the "type" attribute are defined:

- **Individual** – User is allowed to pay for individual content (e.g. PPV or PBT)
- **LocationGroup** 84 - includes aLocation element 50 that specifies the location of the user, which enables, e.g., an evaluation of blackout rules. This is an abstract placeholder for elements that identify a specific type of location (such as country or zip code). A detailed description of this element is provided above in the discussion of Figure 5 (where aLocation is described as a component of the Blackout element). There is also an optional AccessPoint element 88 that, for example, when true ('Y'), indicates that this is the location of an access point that initially obtains the content after the content purchase. In such an embodiment, if this element is false ('N'), then this is the location of a segment of the user's personal network and applies when the user purchased content with the rights to keep a persistent copy and render it on any device within the user's personal network. The default value can be 'Y', for example. When checking if a blackout applies to a user for view-only content, only LocationGroups with AccessPoint set to true (or not present) need to be checked. On the other hand, for content that is to be saved persistently and shared within the user's personal network, all LocationGroups need to be checked. If no LocationGroup is provided, the blackout rules are evaluated as if the user were located everywhere. This means that the user will always be blacked out if blackout rules are specified.
- **aSubscription** element 36 specifies a service or a list of subscription services provided by a given service provider. It is an abstract substitution element that allows for the services and

service providers to be identified using different conventions. A detailed description of this element is found in the discussion of Figure 4, above.

- **GenericRating** element 24 specifies the user-selected content rating ceiling, i.e. the highest level of rating allowed for a given rating dimension. This is an abstract substitution element that allows different rating methods to be used. Authorization for the same user can have multiple GenericRating elements in order to convey the rating ceilings for multiple content rating methods. For detailed description of this element, see the discussion of Figure 6, above.

[0081] The PersistentEntitlements element 90 is illustrated in an example embodiment in Figure 9. Persistent entitlements define the content that a user is entitled to store, either on a hard drive, CD, DVD, or the like for later playback. Such content is referred to as "persistent" because it is stored for later use by the user. This PersistentEntitlements element 90 is the root element of the IPRM Persistent Rights schema. It can either be utilized as a separate XML document that is included inside the SRO along with the Session Rights document, or it can be included directly inside the Session Rights as part of one of the PurchaseOption elements 20 discussed in connection with Figure 3.

[0082] PersistentEntitlements contains the following attributes:

- **renewal** – if, e.g., 'Y', this license may be renewed after it expires. In other words, a request may be sent to a License Server to obtain a new license for already stored content. The rules that would appear in a new license after a renewal can be either taken from one of the renewal

options (see below) or a new set of rules can be obtained (inside an SRO) from an Origin Server.

- **superdistribution** - if, e.g., 'Y', the corresponding content may be superdistributed to other users (which would still have to pay in order to get a valid license for the content). The rules that would appear in a new license associated with a superdistributed copy of the content can be either taken from one of the renewal options (see below) or a new set of rules can be obtained (inside an SRO) from an Origin Server.

[0083] PersistentEntitlements 90 is also a sequence of the following elements, shown in Figure 9:

- **RuleSet element** 92 - a set of content usage rules and restrictions associated with the content, explained in greater detail below in connection with Figure 10.
- **RenewalOption** elements 94 - when the Renewal attribute is set for PersistentEntitlements, each RenewalOption represents a possible set of rules that would go into a new license after a renewal. A RenewalOption also includes a cost, e.g., an amount of money that would be charged to a consumer for renewing a content license with this option.
- **A RuleSet** element 95 of the RenewalOption element 94 has the same type as the RuleSet element of the PersistentEntitlements (see Figure 10). However, in this case the RuleSet represents incremental changes from the original set of rules. When a renewal option is selected, the resulting set of content rules/restrictions is obtained as follows:
  - If a particular rule or restriction is found only in the original (base) RuleSet, copy it into the new PersistentEntitlements.

- If a particular rule or restriction is found only in the RuleSet for the selected renewal option, copy it into the new PersistentEntitlements.
- If a particular rule or restriction is found in both the base RuleSet and in the RuleSet for the renewal option, take the one in the renewal option.
- If a particular rule or restriction is found in neither of the two rule sets, use a default value.

- **The OptionCost** element 96 of the RenewalOption contains both the cost for license renewal using this option and a cost of superdistribution using this option (that may be different from the renewal cost). A more detailed description of OptionCost is provided in connection with Figure 13.
- **Copyright** element 98 - provides copyright information associated with the content.

[0084] The RuleSet element 92 described in Figure 10 sets forth an example of all the rules associated with the specified persistently stored content. (The identity of the content, e.g., a URL, would normally be included in the persistent content entitlements, even though it is not shown in Figure 10).

[0085] A RuleSet element contains a deviceBound attribute, which is a Boolean flag that when set, e.g., to 'Y' means that once a Viewer saves a copy of this content, no further copies of the content may be made, even within the same authorized domain (user's personal network) protected by IPRM security. RuleSet is a sequence with each element (for the exemplary embodiment) as described below.

[0086] The AnalogOutput element 100 restricts copies over an analog interface. It can also define analog proprietary system (APS) parameters, where APS is a mechanism to prevent analog copies of a video signal and would normally be used when the 'copyRestriction' attribute defined below is set, e.g., to NOCOPY (i.e., analog copies are not allowed). An example of an APS is the well known Macrovision system. At the present time, within most commercially available devices, no such equivalent exists for analog audio. Therefore, in most cases when 'copyRestriction' for analog is set to NOCOPY for an audio-only (e.g., music) content, analog output has to be completely disabled.

[0087] The AnalogOutput element 100 consists of the following attributes which apply specifically to analog output:

- **copyRestriction** – an enumeration type that specifies a copy protection state associated with analog interfaces. The IPRM system must ignore (but still preserve) this attribute except in the case when it is exporting content over an analog interface. In that case, the IPRM system must translate this copy protection state to whatever means are available on the particular analog interface (e.g., Copy Generation Management System (CGMS-A) , Macrovision, etc.) This attribute can have one of the following values:
  - UNLIMITED – no limitation on the number of copies of the content that is received over an analog interface.
  - NOCOPY – copying of the content received over an analog interface is not permitted. In practice, this means that when content is transmitted over an analog interface, copy protection (e.g., Macrovision) must be turned on. Some analog video interfaces also support CGMS-A copy protection bits inside VBI.

- NOMORE – no more copies of this content may be made over an analog interface. One way that IPRM-controlled content could get this setting is when (i) the content is imported into the IPRM system over an analog interface, which carries CGMS-A copy protection bits over VBI, and (ii) the CGMS-A relayed over the analog interface was set to ONEGENERATION. Under such circumstances, when the IPRM system imports this content, it is obligated to transition the copy protection state from ONEGENERATION to NOMORE.

- ONEGENERATION –a copy of the content received over an analog interface may be made. When that copy is made, the copy protection state on an external storage device must be set to NOMORE. (The copy protection state kept by the IPRM-protected copy of the content remains unchanged.) It may be possible to relay this copy protection state over some analog interfaces using CGMS-A over VBI.

- numberOfCopies – this attribute is applicable only when copyRestriction attribute is set to ONEGENERATION. In that case, this attribute specifies how many ONEGENERATION copies of the content may be made over an analog interface. A value of zero, for example, can mean that there is no limit on the number of ONEGENERATION copies made.
- **componentOutput** – a Boolean flag. When set, e.g., to 'Y', it is OK to transmit this content over a component analog output.
- **outputAllowed** – a Boolean flag. When set, e.g., to 'N', analog output of any type for this content is disabled. (Component output does not apply to audio-only content, in which case this attribute may be used instead.)

- **pseudoSyncPulse** – a Boolean flag. When set, e.g., to 'Y', the copy protection scheme (e.g., Macrovision) must utilize a Pseudo Sync Pulse (PSP).
- **splitColorBurst** – an enumeration type that can have the following values:
    - N – split color burst not utilized by Macrovision
    - 2 – use 2-line split color burst for Macrovision
    - 4 – use 4-line split color burst for Macrovision
- **constrainedImage** – limits a video image resolution on an analog output. When set, e.g., to 0, there is no restriction on resolution. When set to the opposite state (e.g., 1), an application generating an analog output will decide how to restrict the video image resolution. Otherwise, this attribute specifies a limit on a number of pixels per frame (e.g., in ExCCI, a constrained video image is limited to 520,000 pixels per frame).
- **constrainedAudio** – limits audio bit rate on an analog output. When set, e.g., to 0, there is no restriction on audio bit rate. When set to the opposite state (e.g., 1), an application generating an analog output will decide how to restrict the audio bit rate. Otherwise, this attribute specifies a limit on the bit rate in KBits/sec for analog audio output.
- **audioChannelLimit** – limits the number of audio channels for analog output. When set e.g., to 0, there is no restriction on the number of audio channels. Otherwise, this attribute specifies a limit on the number of audio channels (e.g., if the limit is two, a surround sound audio signal has to be converted to stereo with only two channels).

[0088] The DigitalCompressedOutput element 101 restricts copies over an external digital compressed interface that is not protected with the IPRM system. An example of such an interface would be IEEE-1394 (Firewire bus). However, if there is an IP stack running on top of IEEE-1394 and IPRM is used to protect content over this interface, this element would be ignored.

[0089] DigitalCompressedOutput consists of the following attributes:

- **copyRestriction** – an enumeration type that restricts the number of copies of the content that may be made over an external digital compressed interface. The values of this attribute are defined above in the discussion of the AnalogOutput element 100. This attribute does not apply (but must be preserved) when content is exchanged between devices in the same authorized domain using IPRM security. When content is transferred over an external digital compressed interface, this copy protection state must be translated (e.g., to CGMS-D) and sent over the specific digital compressed interface.
- **outputAllowed** – when this Boolean flag is set, e.g., to 'N', digital compressed content must not be sent over external interfaces even when they are encrypted using a non-IPRM copy protection technology (e.g., 5C). This flag applies when content is sent with an intent to copy as well as when the content is sent with an intent to render-only.

[0090] The DigitalUncompressedOutput element 102 restricts copies of the content that is received over an external digital uncompressed interface (e.g., Digital Video Interface "DVI") that is not protected with IPRM. This element consists of the following attributes:

- **copyRestriction** – an enumeration type that restricts the number of copies of the content received over an external digital uncompressed interface. The values of this attribute are defined above in the discussion of the AnalogOutput element 100. This attribute does not apply (but must be preserved) when content is exchanged between devices in the same authorized domain using IPRM security. When content is transferred over an external digital uncompressed interface, this copy protection state must be translated (e.g., to CGMS-D) and sent over the specific digital uncompressed interface.
- **outputAllowed** – when this Boolean flag is set, e.g., to 'N', digital uncompressed content must not be sent over external interfaces even when they are encrypted (e.g., with High-bandwidth Digital Content Protection (HDCP)). This flag applies when content is sent with an intent to copy as well as when the content is sent with an intent to render-only.

[0091] The Redistribution element 103 defines rules for retransmission of the content beyond the current authorized domain. Note that this element does not apply to super distribution, where a copy of the content is sent to another consumer (in a new authorized domain) without any rights to use the content. This element is used in the cases when an initial set of persistent content entitlements already allows the content to be lawfully shared between multiple authorized domains without an additional cost. The Redistribution element has the following attribute:

- **move** – when this Boolean flag is set, e.g., to 'Y', this content may be moved to another authorized domain. However in the case of a move, all copies of the content in the original authorized domain must be removed. The list of authorized domains to which the content may be moved can be optionally restricted – see below.

[0092] The Redistribution element 103, illustrated in greater detail in Figure 11, includes a sequence of zero or more Destination elements 110, where each destination element allows the content to be copied or moved to that specific destination that is outside of the current authorized domain. Whether or not it has to be a move rather than a copy is determined by the 'move' attribute of the Redistribution element.

[0093] A Destination element contains the following attributes:

- **realm** – identifies another authorized domain to which the content can be copied or moved.
- **id** – a host identifier for a specific device in the specified authorized domain to where the content may be copied or moved. If this parameter is not included, the content may be copied or moved to any device in the specified authorized domain.

[0094] The Redistribution element can also optionally include a GeographicalRestriction element 112 that might prevent movement or copying of content into authorized domains listed in Destination elements, if they are located in blacked out geographical regions.

[0095] The Playback element 104 places restrictions on playback of stored content. It defines conditions which determine when stored content becomes expired and may no longer be used. The Playback element is illustrated in greater detail in Figure 12, and has the following optional attributes:

- **startDate** – the content cannot be accessed before this time.
- **endDate** – the content cannot be accessed after this time.

[0096] A Playback element is a sequence of one or more of the following elements:

- **PlayBackCount** (120) –an integer value that specifies the maximum number of times that this content may be played back before it is considered to be expired. This element has an optional attribute maxDuration that limits the duration of each individual playback. When maxDuration is specified, a playback must be automatically terminated after the specified time period. StartDate and endDate attributes of the Playback element may be used in combination with this element. They would limit the period within which the content may be played in addition to the limit on the number of play backs.
- **Rental** (122) – a choice between EndTime 124 and Interval 126 elements. EndTime is the expiration time for the content after which it must not be usable. Interval is a period of time within which the content is usable and has the following attribute:

  StartOnFirstUse – a Boolean flag. When set, e.g., to 'Y', it means that the rental interval doesn't start until the first time that the content is accessed, e.g., the first time that a decryption key for this content is retrieved from the content license. If this flag value is, e.g., 'N', the rental interval starts when a content license is first created. Once a rental interval is started, the Rental element must be modified with the Interval replaced by EndTime, which is calculated as the starting time of the interval + Interval.

  The startDate and endDate attributes of the Playback element 104 may be used in combination with the Rental element 122 and StartOnFirstUse set to, e.g., 'Y.' They would provide an absolute time interval within which the content may be played in addition to the relative time limit on the period within which content play backs may be started.

- **PauseTime** (128) - max number of minutes of pause time allowed per occasion. What "occasion" means could vary between different rendering applications.

[0097] The MulticastLimit element 105 limits the number of devices that the content can be simultaneously streamed to from a residential home gateway. This does not have to be an IP multicast. If the same content is being streamed to several clients simultaneously over multiple point-to-point connections, that would also qualify as a multicast in this case. A value of, e.g., zero means that the number of such simultaneous devices is unrestricted. Each single multicast of the content is counted as a single playback.

[0098] The Fingerprint element 106 identifies a fingerprint algorithm that is to be inserted into the content as it is being decompressed and delivered over an external analog or digital uncompressed interface. Several Fingerprint elements may be included in order to provide a choice to the rendering device. This element has the following attribute:

- **fingerprintID** – an identifier for a fingerprint algorithm. Any of various known or future fingerprint algorithms may be used. Additional attributes specific to the fingerprint algorithm selected can be provided as necessary, as will be apparent to those skilled in the art.

[0099] The DeviceCapabilities element 107 places some requirements on a device that is allowed to render or store a copy of the content. It has the following attributes:

- **SecurityLevelToRender** – minimum security level of a device required to render this content.

- **SecurityLevelToCopy** – minimum security level of a device required to save a copy of this content. In practice this security level will be greater than or equal to SecurityLevelToRender.
- **CodecInSecureHW** – if this Boolean flag is, e.g., 'Y', a device is required to decompress this content within a secure hardware module.
- **WatermarkInSecureHW** – if this Boolean flag is, e.g., 'Y', a device is required to detect a watermark embedded in this content within a secure hardware module.
- **FingerprintInSecureHW** - if this Boolean flag is, e.g., 'Y', a device is required to insert a fingerprint into this content within a secure hardware module.

[0100] The OptionCost element 96 is a sub-element of a RenewalOption 94 as shown in Figure 9, and identifies the cost of using this option and this set of content usage rules to either renew a license or to buy a super distributed copy of the content. The attributes of OptionCost are:

- **currency** – currency used to specify the cost. A default value of "USD" identifies US dollars.
- **format** – format used to specify the value of the currency attribute, default is ISO4217 (a 3-letter acronym).

[0101] OptionCost element 96, illustrated in greater detail in Figure 13, is a sequence of one or more of the following:

- **RenewalCost** (132) – the cost of renewing a license with this option that contains this set of content usage rules.
- **SuperdistributionCost** (134) – the cost of buying a super distributed copy of the content using this option with this set of content usage rules. When this element and RenewalCost are both present, the same set of

content usage rules may be used for both renewing a license and buying a super distributed copy of the content. The price may be different in the two cases, e.g., a purchaser may get a bigger discount when renewing a license to content already purchased.

[0102] The CopyProtectionRules element 140 is the root element of the IPRM Copy Protection Rules schema, and is illustrated in Figure 14. This element contains copy protection rules associated with forwarding content over output ports and defines rules which are a subset of the rules in IPRMPersistentEntitlements.

[0103] CopyProtectionRules is a sequence of the following elements:

- **AnalogOutput** (100) – restricts copies over an analog interface as described in connection with Figure 10.
- **DigitalCompressedOutput** (101) – restricts copies over a digital compressed interface as described in connection with Figure 10.
- **DigitalUncompressedOutput** (102) – restricts copies over a digital uncompressed interface as described in connection with Figure 10.
- **ForwardingLimit** (142) - limit on the number of simultaneous receivers to which content streams may be forwarded over IPRM-protected connections. A value of, e.g., zero means that content cannot be forwarded.
- **PauseTime** (128) - maximum number of minutes of pause time allowed per occasion. What "occasion" means could vary between different rendering applications. This element is described above in connection with Figure 12
- **Fingerprint** (106) - identifies a fingerprint algorithm that is to be inserted into the content as it is being decompressed and delivered over an external analog or digital uncompressed interface. Several Fingerprint

elements may be included in order to provide a choice to the rendering device. This element is described above in connection with Figure 10.

[0104] Figure 15 is a block diagram illustrating an example network environment in which the invention can be used. A content provider 150 provides digital content via a communications network 151 such as the Internet. The content may be provided, for example, as streaming media. Upon receipt of the content, a home gateway 152 can decrypt the content (if decryption is authorized) and apply the IPRM rules to the content. If authorized for copying, the content can be copied onto a DVD writer 155, or the like. As will be appreciated by those skilled in the art, other copying means may be provided, such as a CD writer, video tape recorder, etc. Licensed content may also be stored locally, e.g., on a hard disk drive 156. Other types of storage media currently known or developed in the future may additionally or alternatively be provided for storing licensed content to be played at a later time.

[0105] Various video, audio and/or multimedia appliances may be coupled to the home gateway for reproduction and/or storage of licensed content. Such devices, referred to as device N and device N+1 are illustrated in Figure 15 as devices 153 and 154. These may be analog or digital devices which are permitted or denied access to particular content based on the IPRM rules applied by the home gateway 152, e.g., in accordance with XML documents as described above. Any number of such devices within the hardware and/or software capabilities of the particular home gateway 152 may be provided.

[0106] A home network 157 is also coupled to the home gateway 152 to distribute content to appliances (e.g., PCs, televisions, PVRs, CD/DVD players, etc.) coupled to the home network. The home network 157 may be any type of available network, including wired and wireless (e.g., any of the IEEE 802.11 Wi-Fi standards, Bluetooth, etc.).

The home network 157 may also be coupled, via a suitable gateway 158 as well known in the art, to other authorized networks 159. Such a network 159 may comprise, for example, another home network to which the subscriber at home network 157 is authorized to forward licensed content. This can be useful, for example, where the subscriber at home network 157 has a second (e.g., vacation) home where it is desired to view content.

[0107] It should now be appreciated that the present invention provides methods for IP rights management within an authorized domain. The methods provide flexibility in that rules for separate systems do not have to be tied together. Instead, a universal set of rules is provided to enable rights management in an authorized network that may include many different products, including both analog and digital video, audio, and multimedia appliances. Moreover, rules are provided for both streaming content and locally stored content.

[0108] While the present invention has been shown and described with reference to the preferred mode as illustrated in the drawings, it will be understood by those skilled in the art that various changes in detail may be effected therein without departing from the spirit and scope of the invention as defined by the following claims.